verifying by calculation and comparison in the device (3) of the said first result (O_AC_I) of an irreversible function (OWF) and of that received from the medium (1), wherein, if the said comparison and verifications each give equality, an acceptance and a storage by the device (3) of the electronic cheque issued by the medium (1), thereby, allowing the devise (3) to recognize the authenticity of the medium (1) and of the cheque being received.

## Remarks

**Rejections under 35 U.S.C. § 112, first paragraph**

Claims 1-22 stand rejected under 35 U.S.C. § 112, first paragraph. The Examiner has asked the Applicants to describe how the invention is to be utilized in the Figures and Specification beyond what has been submitted.

The invention as submitted in the specification and set forth in the claims is directed towards a method of payment by electronic cheques. In most modern electronic payment schemes, consumers make use of a banking card to perform payment transactions with merchants that have some sort of card accepting device. For reasons of cost or transaction time, often these transactions are conducted off-line, *i.e.,* without making a connection to the bank of the cardholder or that of the merchant. Moreover, globalization has made interoperability between different payment schemes a new challenge for financial institutions.

The off-line and interoperability requirements in combination with the risk of fraud have lead the financial institutions to initiate the migration from magnetic strip cards to smart cards. Smart cards contain a small processor and are capable of storing

data, keeping cryptographic keys and performing cryptographic computations. The present invention organizes the interoperability between the electronic cheques and reading devices.

The Examiner has requested that Applicants delineate how to enable and realize the best mode of the invention. Applicants submit that the best mode for operation of the invention is disclosed in the specification. Additionally, Applicants respectfully submit that the specification as submitted provides sufficient enabling disclosure as required under 35 U.S.C. § 112, first paragraph, so that one of ordinary skill in the art could re-create the invention.

For example, Figures 1, 4, 5 and 6 and respective accompanying written disclosure in the specification, provide illustration and explanation of how various components, *e.g.,* cheque cards, readers, financial institutions, etc., of the invention operate to achieve recognition of the authenticity of electronic cheques.

Further, Figures 2 and 3 and respective accompanying written disclosure provide explanation of the underlying principles and algorithms upon which the invention is based. The invention makes use of various cryptographic and irreversible functions to achieve recognition of the authenticity of electronic cheques. Cryptographic and irreversible functions, or one way functions, *See* p.14, ln.15., are generally known to those of ordinary skill in the art. Applicants respectfully submit that the novel relationships between the various functions are disclosed and described in the specification so that one of ordinary skill in the art could re-create the invention. *See generally* pp. 13-22 of the specification and specific citations listed hereinbelow.

To assist the Examiner with understanding the enabling aspects of the disclosure and what is claimed, Applicants have amended claim 1 for clarity and to conform with traditional U.S. claim writing practice. The amendment to claim 1 is for clarifying purposes only, and thus, does not change the scope of the claim and is not a narrowing amendment.

Applicants respectfully submit that independent claim 1, as amended, is fully enabled by the specification as required by 35 U.S.C. § 112, first paragraph. Thus, Applicants respectfully traverse this rejection and request reconsideration and withdrawal of rejections of claims 1-22 under § 112, first paragraph.

**Rejections under 35 U.S.C. § 112, second paragraph**

Claims 1-22 stand rejected under 35 U.S.C. § 112, second paragraph, as being indefinite. To facilitate the Examiner's understanding of the claimed invention, Applicants have amended the language of claim 1. Applicants respectfully submit that claim 1, as amended, provides sufficient basis to particularly point out and distinctly claim the subject matter which Applicants regard as the invention as required under U.S.C. § 112, second paragraph.

The Examiner has requested that Applicants define a list of claim elements to permit one to evaluate what Applicants regard as their disclosure. Applicants respectfully submit that all of the claim elements set forth in the claims are adequately defined in the disclosure to meet the requirements of § 112, second paragraph. Many of the elements that the Examiner has requested further definition of are based upon various known concepts related to cryptographic or irreversible functions. *See* p.13 ln.37 – p.14

ln.2. As is known in the art, an irreversible function converts an input and a diversification parameter to an output. The detailed description of the inputs and parameters of the irreversible functions preferably used by the invention can be found at p.16 lns.1-27.

As disclosed in the application, the invention uses these various functions to achieve interoperability between electronic cheques and reading devices. To demonstrate that the claim elements have been sufficiently defined to meet the requirements of § 112, Applicants have provided reference to corresponding support in the specification.

The Examiner has asked for the "precise calculations of table 5" and the "nature of an irreversible function". The calculations used in table 5 are cryptographic functions and defined on pp. 13 and 14 of the specification. As discussed above, irreversible functions are known to those skilled in the art.

The Examiner has asked for further definition of the "calculation of the secret key (K) by algorithmic delineation", "the calculation of the distinctive sign (IMcf)", and "a first result (O_AC_I) of the irreversible function". The relationship between these concepts is disclosed in the specification at p.19 lns. 10 – 25.

The Examiner has asked for definition of the "processed result (AC_I) of the first algorithm (MAC) together with mathematical description of the secret verification key (SVK) and description of the dynamic parameters (CDP) of the cheque as well as description of the second iteration transformation". These concepts are disclosed and defined at p.17 ln. 36 – p.18 ln. 20.

The Examiner has asked for the "the methodology of the pseudo random estimation by the device (3), the result (AC_I) and the base values S(!)....S(k)". These concepts are disclosed and defined at p.18 ln. 25 – p.19 ln. 10.

The Examiner has asked for the "comparison process of the distinctive sign (IMcf) and a verification in the device(3) of the second result (AC_C)". These concepts are disclosed and defined at p.19 lns.10 – 30.

The Examiner has asked for "the discussion of the equality condition for acceptance and discussion of the summing condition for odd or even products of number, n, k together with discussion of the digital signature (SIGNcr)". This discussion is disclosed and defined at p.18 ln.29 – p.19 ln.2.

Applicants respectfully submit that the invention as set forth in amended claim 1 and the accompanying specification meets all the requirements of 35 U.S.C. § 112, second paragraph. As shown above, all of the claim elements that the Examiner requested clarification for are clearly supported and defined by the specification. Additionally, Applicants have revised claim 1 to make what is claimed more clear. As amended, the language of the claim now conforms with traditional U.S. claim writing practice. Applicants respectfully request reconsideration and withdrawal of the § 112 rejections, second paragraph, of claims 1-22.

## CONCLUSION

In view of the above, it is respectfully submitted that all claims are in condition for allowance. Applicants respectfully request allowance of all rejected claims.

A check for $400.00 is attached for a two-month extension of time. The Commissioner is hereby authorized to charge any additional fess created by this response or credit any overpayment to Deposit Account Number 04-1425, referencing attorney docket number 5453.00 and client matter number 443502-0001. A duplicate of this Amendment is enclosed for that purpose.

Should the Examiner have any questions or suggestions that may advance the instant application toward allowance and issuance, Applicants respectfully request that the Examiner call Applicants' representative indicated below in such furtherance of prosecution.

Respectfully submitted,

Date: October 15, 2002

By: _____

Sean. S. Wooden, Reg. No. 43997
Dorsey & Whitney LLP
1001 Pennsylvania Avenue, N.W.
Suite 400
Washington, D.C. 20004
Tele: (202) 442-3000
Fax : (202) 442-3199

Attachment: (Version With Markings to Show Changes Made)

**Version With Markings to Show Changes Made**

1. (Amended) Method of payment by electronic cheque [, in particular in the case of a direct transaction] between [solely:] a payment issuer furnished with a medium (1) comprising at least one blank electronic cheque certified by a financial institution (BA) and an overall amount useable at least partially in respect of the electronic cheque, and, a recipient of the payment furnished with a device (3) adapted to receive at least one aforesaid electronic cheque of the abovementioned medium (1), [the] said method comprising the steps of:, [so that the devise (3) can recognize the authenticity of the medium (1) and of a cheque being received,]

[a] calculating [calculation] by the medium (1) of a table (5), possibly partial, on the basis of at least one set of k base values (S[1], . . . S[k]), by applying successively to each of them n times an irreversible function (OWF) with parameter(s) differing preferably with each application and giving k intermediate values n times;[, ]

[a]calculating [calculation] by the medium (1) of a secret key (SK) on the basis of the last k intermediate values of order n and, on the basis of this key (SK), a calculation of a distinctive sign ($IM_{cf}$) of the cheque;[,]

[a transmission] transmitting by the medium (1) to the devise (3) [of] the distinctive sign ($IM_{cf}$) calculated for the electronic cheque;[,]

generating a financial commitment [of] by the medium (1) in relation to the device (3), as regards the cheque by supplying to the device (3):[,]

a first result (O_AC_I) of an irreversible function (OWF) via which was processed the result (AC_I) of a first algorithm (MAC) combining a secret verification key (SVK), originating from the financial institution (BA) issuing the electronic cheque, and dynamic parameters (CDP) of this cheque, and

a second result (AC_C) of a second algorithm (MAC) combining the secret key (SK) calculated for the medium, the dynamic parameters (CDP) of this cheque and the first result (O_AC_I) hereinabove;[,]

generating by the device (3), at least one random/pseudo-random guesstimation [, by the device (3),] of k numbers m of successive applications of the irreversible function (OWF) to the k base values (s[1],...S[k], the k numbers m lying between zero and n and possibly being different from one another, the sum of the k numbers m having to be a determined constant;[,]

[a transmission] transmitting by said device [of] the result of the guesstimation [by the device (3)] to the medium (1);[,]

[a response] responding by the medium (1) to [the] said guesstimation by the device (3), comprising [on the one hand,] the result (AC_I) of the first algorithm combining the secret verification key (SVK) and the dynamic parameters (CDP) of the cheque and, [on the other hand,] a set of the k intermediate values obtained during the successive applications of the irreversible function (OWF) to each of the k base values (S[1],...S[k]) the number or numbers of times m lying between zero and n;[, ]

[-by the device (3):]

[successive applications] successively applying, by said device, [ of] the irreversible function (OWF) to each of the k intermediate values of order(s) m until the last k intermediate values of order n are obtained;[,]

[calculation] calculating of the said secret key (SK), by said device, on the basis of these last k intermediate values of order n and, on the basis of this secret key (SK), a calculation of the distinctive sign ($IM_{cf}$) of the cheque;[,]

[a comparison of] comparing, by said device, the distinctive sign ($IM_{cf}$) thus calculated and of the distinctive sign ($IM_{cf}$) calculated by the medium (1) and received from the latter;[,]

[a verification] verifying by calculation and comparison in the device (3) of the said second result (AC_C) of the second algorithm (MAC) and of that received from the medium (1);[,]

[a verification] verifying by calculation and comparison in the device (3) of the said first result (O_AC_I) of an irreversible function (OWF) and of that received from the medium (1); wherein,[and,] if the said comparison and verifications each give equality, an acceptance and a storage by the device (3) of the electronic cheque issued by the medium (1), thereby, allowing the devise (3) to recognize the authenticity of the medium (1) and of the cheque being received.